



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

# Secure Network Design: Micro Segmentation

*GIAC (GSEC) Gold Certification*

Author: Brandon Peterson, brandonp@dri.edu

Advisor: Stephen Northcutt

Accepted: February 5, 2016

## Abstract

Hackers, once on to a network, often go undetected as they freely move from system to system looking for valuable information to steal. Credentials, intellectual property, and personal information are all at risk. It is generally accepted that the attacker has the upper hand and can eventually penetrate most networks. A secure network design that focuses on micro segmentation can slow the rate at which an attacker moves through a network and provide more opportunities for detecting that movement. Organizations that implement a secure network design will find that the added cost and complexity of micro segmentation is more than offset by a reduction in the number and severity of incidents. In fact, the effort extended in learning, classifying, and segmenting the network adds value and strengthens all of the organization's controls.

## 1. Introduction

Secure network design or architecture begins with the understanding that most business processes require network communication to traverse untrustworthy networks. Certainly the Internet qualifies, but even the business's own internal networks may be unsafe. Insider threats, hackers in the network, and unintended data leaks are constant threats an organization must anticipate and prepare for. As the world becomes more connected business risk will increase, "a huge online population means that even attacks with very low success rates will have significant pools of victims" (Herley, 2014, p. 70). A 2011 survey by the Ponemon Institute found that 80% of the 583 survey responders believed their organization's network security had suffered at least one breach in the last twelve months. IT security professionals from all sizes of companies, both the private and public sector, and a variety of different industries illustrates that the problem is widespread (Ponemon Institute, 2011).

The costs of cyber-crime to business are also high. Determining the exact cost of cyber-crime is tricky, considering the numerous factors involved and the lack of information. McAfee and the Center for Strategic & International Studies, in 2014, estimated the annual cost at over \$400 billion globally (McAfee, 2014).

With the cost, surface area, and volume of attacks so high, it is more critical than ever to protect the organization's interests with a secure network design focused around micro segmentation. Micro segmentation, also known as protected enclaves, protect the network by breaking it into smaller chunks. This is accomplished through the use of network firewalls, host firewalls, VLANs, VPNs, and Network Admissions or Access control (Northcutt, 2007). These techniques add complexity and cost to managing a network. Fortunately, new technology is emerging that can ease the burden and cost of these implementations.

## 2. Determining Enclave Boundaries

With the advantage of time hackers can float throughout a network for months looking for additional access or data to steal. By micro segmenting the network, an organization creates boundaries that the attacker has to cross before gaining access to another subset of data. These boundaries are created in a way that only allows the minimum necessary services through. These services are then closely monitored to detect any unauthorized use.

Determining what boundaries or VLANs to create and what resources should be placed in those boundaries is one of the more challenging aspects of designing a secure network. In general, the need for an enclave arises “when the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment.” (Rome, 2001). A value threshold should also play a role in selecting enclave boundaries. For example, an e-commerce website may want to separate their webserver handling their store operations from a webserver handling their jobs and recruiting page. Both sites may require 24/7 availability and contain sensitive information, however, the e-commerce site represents a far greater impact on business operations if its availability is negatively impacted. ERP applications are another example of high value applications that deserve their own segment. The organization’s workflow may dictate that additional services be segmented. Email, file shares, and custom applications may all justify segmentation.

A good measure of business impact for a system can often be found in an organization’s disaster recovery or business continuity plans. These plans often provide details on the priority of systems or data. Figure 2-1 shows a sample Recovery Objectives table from a disaster recovery plan.

System Name	Recovery Point Objective	Recovery Time Objective
Email	2 hours	24 hours
E-Commerce Website	0	>10 seconds
Intranet	7 days	14 days
Payroll	8 hours	3 days

*Figure 2-1 Disaster Recovery Objectives Table*

The table makes it clear that these systems all have different value to the organization. At a minimum, a segment for the E-Commerce Website should be considered.

Another key segmentation line is around compliance. It is far easier to manage compliance if the number of systems under scope can be reduced through segmentation. While segmentation is not strictly required for PCI compliance, “Without adequate network segmentation (sometimes called a “flat network”) the entire network is in scope of the PCI DSS assessment.” (PCI Security Standards Council, 2015). The PCI requirements document has a flowchart for determining if card holder data is segmented and scope can be reduced. Clearly, it benefits the organization to segment when compliance is involved.

Physical security can play a role in determining if another segment is needed. For example, imagine an office building with 100 identical workers spread across two floors. The bottom floor is in an area with access to the public. The top floor only allows employee access. The information on all 100 systems has the same value and security needs. However, the additional risk presented by the physical access to the systems on the bottom floor means that additional controls are necessary. Network segmentation should be one of the controls considered.

Wireless should be considered another segmentation qualifier. Due to the fact that it is nearly impossible to physically secure a wireless network, they should be segmented on a private VLAN. On a private VLAN, attached devices are not able to directly communicate with each other. This helps prevent compromised systems and rogue users from spreading to other systems on the wireless network.

Figure 2-2 shows the enclave boundaries flowchart that may help network administrators decide when to create a segment.

### 3. Network Access Control

Once an enclave is created, it is important to ensure that only approved devices are granted network access. Network Access Control or NAC refers to technology that restricts network access to devices that meet certain policy controls (e.g. anti-virus software, patch level, host firewall), provide sufficient user credentials, or match a certain physical (MAC) address.

802.1x Port-Based Network Access Control allows clients to authenticate using credentials such as passwords or certificates to gain network access. The client sends an authentication request to the switch using the Extensible Authentication Protocol over LAN (EAPOL). EAPOL allows an EAP request to be encapsulated and transmitted over Ethernet. The switch acts as a proxy and takes the encapsulated EAP request and converts it into a RADIUS request, sending it on to the authentication server. The responses returning from the authentication server are then converted back into EAPOL for the client. These transmissions happen until the client is approved or rejected by the authentication server. Once approved, the port on the switch is activated and the client is assigned a VLAN ID. (Cisco, 2009). Unapproved devices may be segmented into a guest VLAN or denied network access.

For devices such as printers, scanners, copiers, etc. that don't have the capability to do 802.1x authentication, there are a couple of options that can be used depending on the

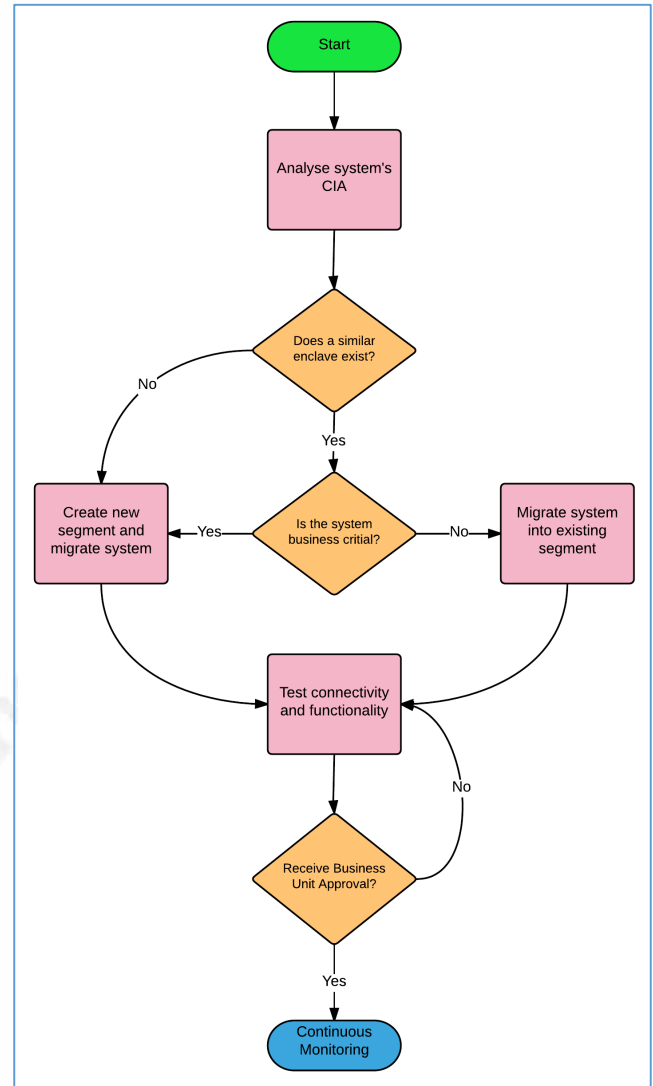


Figure 2-2 Micro Segmentation Decision Flowchart

scale of the network. One option is to simply use port security to lock down the port on the switch to a specific MAC address. This method becomes cumbersome if used on more than a handful of devices. Another option is to use MAC Authentication Bypass or MAB. “Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.” (Cisco, 2009). MAB can be configured as a failover method of authentication should 802.1x fail. In MAB, the device’s MAC address is used as the credentials to authenticate with.

After the device has been authenticated and assigned to a VLAN, the DHCP server can be setup to only assign IP addresses for known MACs. While a static IP address assignment easily bypasses this control, it does help prevent users from sharing credentials. Figure 3-1 shows the first two phases of a device as it connects to the network in a NAC environment with DHCP MAC filtering.

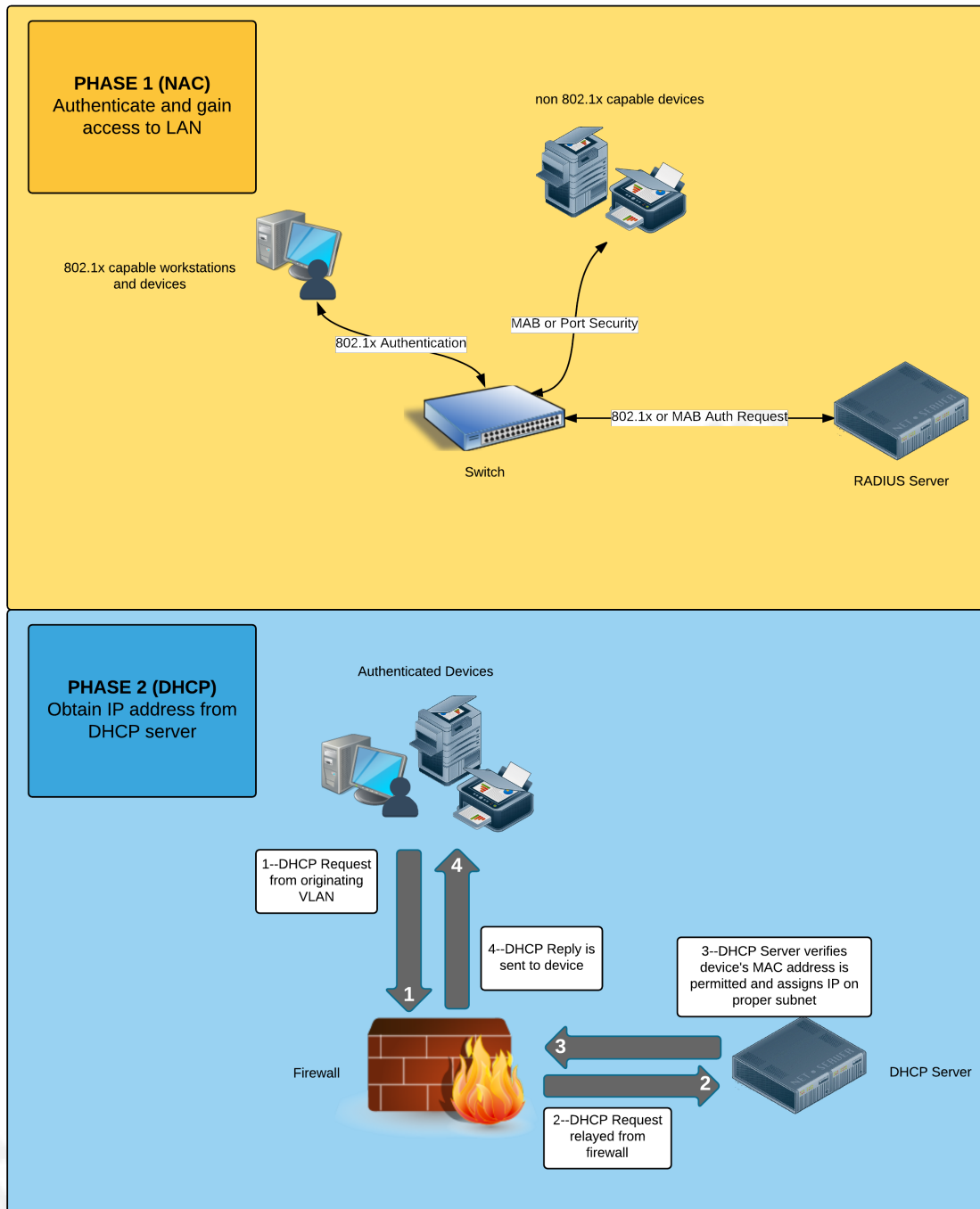


Figure 3-1 NAC and DHCP filtering combined

Many different vendors offer proprietary PNAC solutions that extend the IEEE 802.1x protocol further. They offer capabilities like dynamic VLAN assignment, anti-virus, and patch scanning. Dynamic VLAN assignment allows users to take a laptop, for instance, to another part of the network and be automatically assigned to their correct

VLAN. Patch and anti-virus scanning ensures that machines are in compliance with corporate security policies. Machines failing the compliance check are connected to a quarantined VLAN until the machine is brought back into compliance. Most solutions also offer the ability to send unknown machines into a guest VLAN. This allows guests to gain limited network access without having to tie up limited IT resources.

This may not be enough on its own, unfortunately, to prevent rouge machines or individuals from gaining network access. Spoofing MAC addresses is trivial. User credentials can easily be stolen or purchased on the black market. At DefCon 19, Alva Duckwall IV demonstrated defeating 802.1x using a Linux machine as a bridge. (Duckwall, 2011). Previously at BlackHat 2007, Ofir Arkin gave a presentation on bypassing NAC. His methods included purposely getting a machine quarantined in order to infect other machines in the quarantined area. The legitimate machines would likely eventually be brought back into the network with his malware intact. (Arkin, 2007).

### 3.1. Rouge Device Detection

Not all organizations have the resources to properly implement Network Access Control to automatically restrict devices from connecting to the network. Frequently, even networks that use NAC have enough exceptions that they still need a tool to help notify them of devices that connect to the network.

Arpwatch is a free open source tool developed by the Network Research Group at Lawrence Berkeley National Laboratory. It monitors the network for MAC and IP address pairs. Arpwatch sends an email alert when it notices a new pair, a pair that has not been used for 6 months or longer, and if a MAC or IP address is detected associated with a different MAC or IP. In figure 4-5, an email from Arpwatch alerts administrators to an IP address associated with two different MAC addresses within a short period of

time.

```

From: ArpWatch [mailto:arpwatch@company.local]
Sent: Thursday, December 31, 2015 12:13 PM
Subject: changed ethernet address (linux-server.company.local)

hostname: linux-server.company.local
ip address: 10.10.14.59
ethernet address: 0:50:56:b0:72:e4
ethernet vendor: VMware, Inc.
old ethernet address: f8:b1:56:d8:50:68
old ethernet vendor: Dell Inc.
timestamp: Thursday, December 31, 2015 12:12:55 -0800
previous timestamp: Wednesday, December 30, 2015 12:28:08 -0800
delta: 23 hours

```

*Figure 3-2 ArpWatch email alert*

In the case of the rouge device such as a rouge wireless access point attaching to the network, Arpwatch would detect a new pair to new MAC associated with an existing IP. The network or security administrators could then determine if the device is approved and inventoried. If not, appropriate action such as removing the device or determining if an incident has occurred should take place.

Network Access Control is not a silver bullet; it is just another layer to aid in the fight. It needs to be combined with a good understanding of your network traffic and monitoring.

## 4. Monitoring

Network segmentation is effective at slowing an attacker as he moves across the network. Unfortunately, it alone does not stop an attacker. It has been well publicized that the average attacker is present on a network for over seven months before initial detection. Furthermore, most of the initial discoveries were made by entities external to the affected companies (Mandiant 2014 Threat Report). A skilled penetrator will determine what ports and services are open between segments and patiently work his way across until he discovers something of value: credentials, personal information, intellectual property, etc. Therefore, it is important to understand what constitutes normal business traffic on the network and to detect deviations from the norm.

The associated ports, protocols, and applications used to conduct business should be documented. This makes it possible to then detect outliers or rouge processes. In

figure 4-1, dropped VNC traffic for a department that only uses web surfing, file sharing, and email should be investigated.

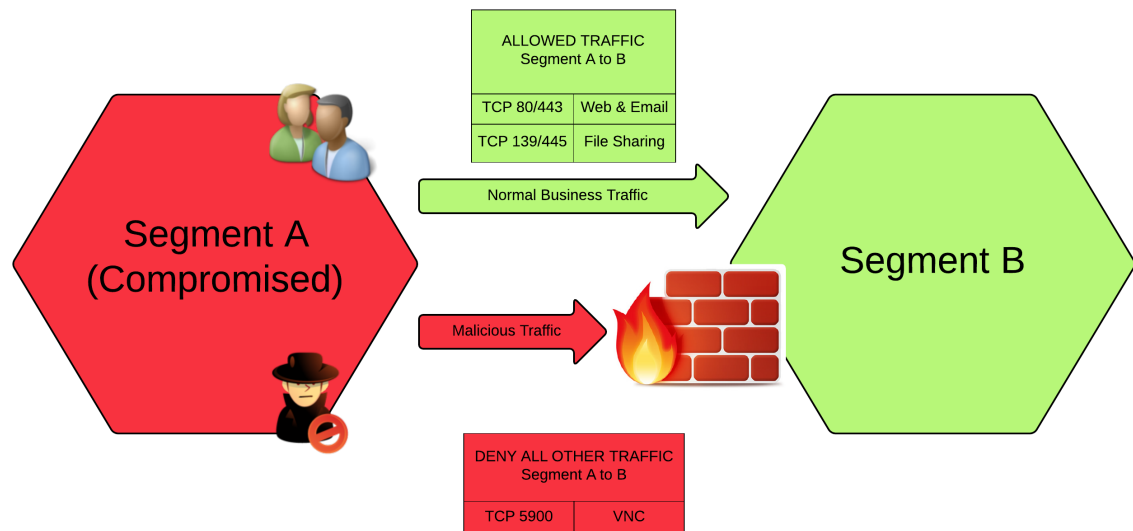


Figure 4-1 Compromised Network Segment

Tight network controls force the hacker to use the channels available to them. To the untrained eye, the traffic seems to normal—a part of the permitted business traffic. Known as covert channels, clever attackers find ways to blend in with the normal business channels to transmit their payloads. DNS is a perfect example of a nearly ubiquitous service that can be used as a covert channel. Using an encoding scheme such as base32, a covert channel can be used to transmit binary information through DNS. The encoded data is sent in the form of a DNS query. The leftmost or host side of the query contains the embedded data. The authoritative name server which is controlled by the hacker then returns data embedded within a DNS txt record. This equates to roughly 150 bytes of arbitrary data exfiltrated and considerably larger sums embedded in the returning txt record. Using this technique, researchers were able to achieve data transfer speeds as high as 150KB/s (Faldella & Tucci). In practice, understanding that most segments don't require recursion for txt records or queries on longer hostnames can help you configure your name servers securely or catch such requests as they traverse the network.

With a policy in place that details acceptable business use and an understanding of the underlying technology a network security administrator can begin to apply controls to monitor and detect deviations.

#### 4.1. Network Monitoring Architecture

To facilitate network level monitoring, organizations need to ensure they budget for and include monitoring hardware and software as they build out the network. The goal is to duplicate enough of the traffic at critical locations to catch anomalies. On a small scale, this can be accomplished simply by mirroring ports on the switch or inserting a network tap. Most organizations will eventually overload their monitoring and security scanners with critical feeds they wish to monitor. Figure 4-2 depicts the issue of aggregating too many feeds into a scanner.

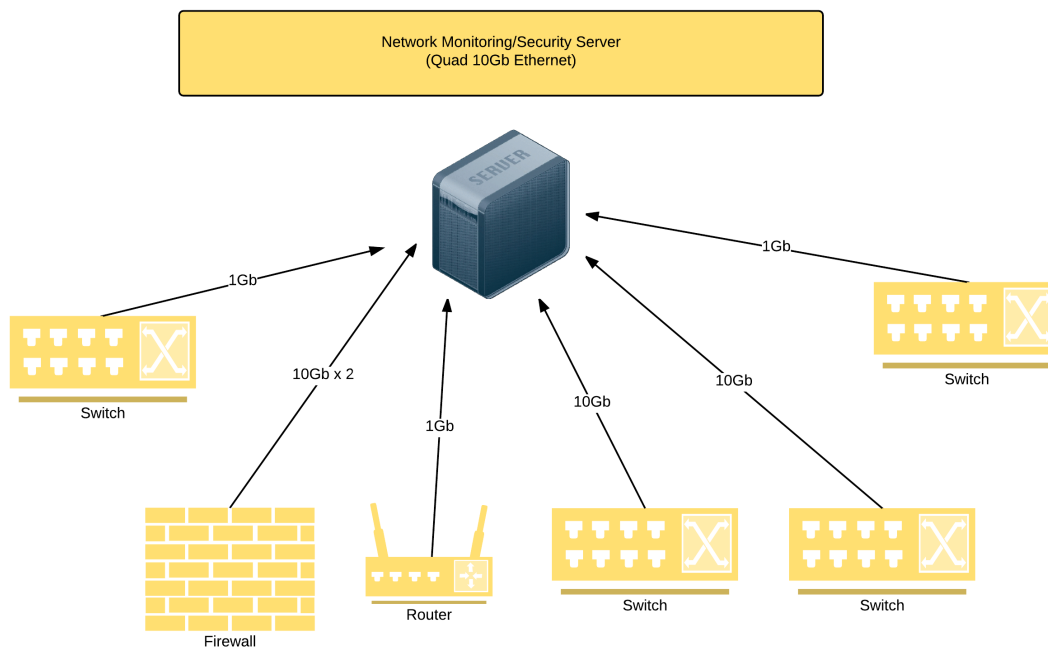


Figure 4-2 Aggregate Network Monitoring Feeds

It is readily apparent in this example that even with a quad 10Gb Ethernet card there is potential to overload the server. Investing in additional hardware at the monitoring server quickly becomes cost prohibitive.

Several network vendors have come up with a solution to this problem. Gigamon, one of the leading makers of network visibility sells products to create what they call Visibility Fabric™. (Gigamon, 2016). Rather than send all the tap feeds and mirror ports

directly to the server, they are sent to a device that first processes the network traffic. These devices can de-duplicate traffic, strip headers or payload off the packets, decrypt encrypted traffic, generate Netflows, and more prior to sending the traffic on to the monitoring server. Another useful feature they share is the ability to aggregate multiple feeds into one. This allows the server to process many times the network traffic it would otherwise be able to handle. As networks speeds get faster and the number of connections grow the need for network level aggregators and packet manipulating devices will increase. “Forecasts from analyst firms such as Gartner, Frost & Sullivan and others paint a clear picture of the significant growth we can expect in the network monitoring space over the next few years” (O’Donnell, 2014).

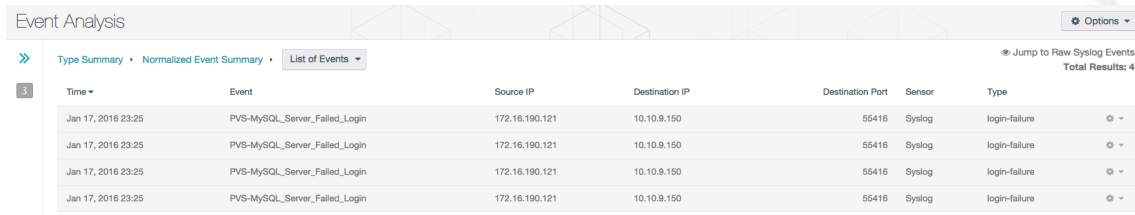
## 4.2. Detection

Once the network traffic is aggregated it can be sent to a number of different monitoring and security products for inspection. For example, Tenable’s Passive Vulnerability scanner can detect new hosts on the network, identify vulnerabilities in both client and server side traffic, and detect other anomalies. Figure 4-3 shows the top 20 anomalous events detected by Tenable’s PVS on a sample network.



Figure 4-3 Tenable Passive Vulnerability Scanner Events

Drilling down into the “login-failure” event shows the details of traffic that triggered the event. As seen in figure 4-4, Tenable’s PVS detected several failed login attempts to a database between two segments on the network.



The screenshot shows the 'Event Analysis' interface with a tab for 'List of Events'. It displays a table of four failed login events. Each event occurred on Jan 17, 2016 at 23:25, originating from 172.16.190.121 and targeting 10.10.8.150 on port 55416. The sensor used was Syslog, and the event type was 'login-failure'.

Time	Event	Source IP	Destination IP	Destination Port	Sensor	Type
Jan 17, 2016 23:25	PVS-MySQL_Server_Failed_Login	172.16.190.121	10.10.8.150	55416	Syslog	login-failure
Jan 17, 2016 23:25	PVS-MySQL_Server_Failed_Login	172.16.190.121	10.10.8.150	55416	Syslog	login-failure
Jan 17, 2016 23:25	PVS-MySQL_Server_Failed_Login	172.16.190.121	10.10.8.150	55416	Syslog	login-failure
Jan 17, 2016 23:25	PVS-MySQL_Server_Failed_Login	172.16.190.121	10.10.8.150	55416	Syslog	login-failure

Figure 4-4 Tenable Passive Vulnerability Scanner Event Details

Without segmentation, this traffic would have remained “hidden” on the local subnet. Segmentation forces the traffic to cross key junctions where the traffic can be captured and analyzed.

### 4.3. Vulnerability Scanning

It is important to validate your security controls such as patching, secure baseline configurations, and proper user access rights. Vulnerability scanners are able to scan a variety of different devices on the network for insecure software or configurations. They can also aid in detection of rogue devices on the network.

Micro segmentation allows you to derive more value out of a vulnerability scanner by tailoring scans to match the micro environment. Figure 4-6 shows a page

from a Nessus report targeted to a PCI scoped segment.

192.168.1.28					
Summary					
Critical	High	Medium	Low	Info	Total
1	4	12	5	20	42
Details					
Severity	Plugin Id	Name			
Critical (10.0)	33850	Unsupported Unix Operating System			
High (9.3)	22466	OpenSSH < 4.4 Multiple Vulnerabilities			
High (7.5)	44077	OpenSSH < 4.5 Multiple Vulnerabilities			
High (7.5)	44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass			
High	33929	PCI DSS compliance			
Medium (5.9)	31737	OpenSSH X11 Forwarding Session Hijacking			
Medium (5.8)	44081	OpenSSH < 5.7 Multiple Vulnerabilities			
Medium (5.8)	56283	Linux Kernel TCP Sequence Number Generation Security Weakness			
Medium (5.5)	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass			
Medium (5.4)	17744	OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing			
Medium (5.0)	12213	TCP/IP Sequence Prediction Blind Reset Spoofing DoS			
Medium (5.0)	17704	OpenSSH SKEY Authentication Account Enumeration			
Medium (5.0)	67140	OpenSSH LoginGraceTime / MaxStartups DoS			
Medium (4.6)	44076	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection			
Medium (4.3)	17705	OPIE w/ OpenSSH Account Enumeration			
Medium (4.0)	17703	OpenSSH < 5.9 Multiple DoS			
Medium (4.0)	44065	OpenSSH < 5.2 CBC Plaintext Disclosure			
Low (3.5)	19592	OpenSSH < 4.2 Multiple Vulnerabilities			
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled			
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled			
Low (2.1)	53841	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure			
Low (1.2)	44080	OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking			
Info	10114	ICMP Timestamp Request Remote Date Disclosure			
Info	10267	SSH Server Type and Version Information			
Info	10287	Traceroute Information			
Info	10662	Web mirroring			
Info	10881	SSH Protocol Versions Supported			
Info	11032	Web Server Directory Enumeration			
Info	11219	Nessus SYN scanner			

Figure 4-5 Nessus PCI Compliance scan

The machine in the scan did not meet compliance requirements. The Nessus reports details why the device fails and contains information on how to fix the issues.

In some cases, organizations find it useful to create custom scans for their unique environment. Many organizations have developed and deployed custom applications. For instance, a custom scan could be written to track the version of a custom application. If a particular version of the custom application has issues, support staff would know which machines had the trouble versions.

## 4.4. Data Loss Prevention

Data Loss Prevention (DLP) tools help organizations “discover, classify and monitor sensitive information, wherever it’s stored or used, on and off of corporate networks.” (Blevins, 2014, p. 13). This is technically accomplished in a variety of

different ways depending on the solution. Email, web, endpoints, databases, and even social networks can be scanned for data classified as sensitive. Micro segmentation aids DLP implementations by shrinking the surface area to monitor and assisting in the classification of data. As an example, in a micro segmented network, it may not be necessary to scan a custodial segment for HIPAA or PCI data. This helps target DLP where it is most useful and should keep licensing and implementation costs lower. “Installing DLP on everything, everywhere can be very expensive and difficult to maintain. Think about the key applications and teams within your business that really need DLP technology due to the sensitivity of the data they have access to.” (Dalton, 2014).

#### **4.5. Compliance**

The regulatory and compliance requirements organizations operate in continue to change as the threat landscape evolves. PCI DSS, HIPAA, and SOX have all undergone changes in the last few years and added additional requirements. Micro segmenting typically allows organizations to limit the scope of compliance requirements. This becomes necessary in most organizations because compliance is expensive to enact across an entire organization. “In such instances, it's reasonable to consider moving the PCI systems into their own dedicated environment and limiting their interaction with non-PCI technology. This helps reduce the number of critical systems to be reshaped into compliance and will enhance security by placing them in a controlled and monitored environment.” (Mundhenk & Rothke, 2007).

In addition to limiting the scope of compliance, an effective micro segmentation implementation will satisfy many compliance requirements without additional work. The environment will already be well documented. Also, several layers of security controls including monitoring and vulnerability scanning will be in place.

### **5. Incident Response**

Micro segmenting a network provides advantages when dealing with incidents. The extra layer of monitoring makes identification of an attack or breach easier to detect.

Once detection has occurred the subsequent phases of incident response are also made simpler by micro segmentation.

## 5.1. Containment

Containing a threat or attacker before they have the opportunity to do more damage or spread on the network is critical. An entire segment can be quickly isolated to contain a threat, as in Figure 5-1.

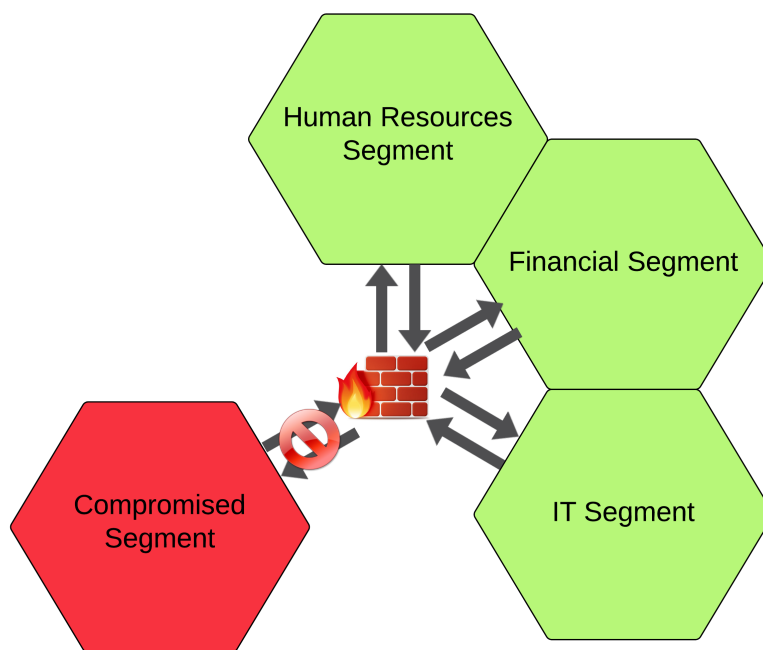


Figure 5-1 Traffic from compromised segment is easily isolated

Since the segment sizes are relatively small, there are fewer business units affected by the interruption of service.

If containment is limited to just a few machines within a micro segment, the network architecture lends itself to rapid isolation. Most micro segmentation is accomplished through the use of 802.1Q tagging. An “Isolation VLAN” can be created throughout the network before hand that only incident responders can access. This allows network administrators to easily and remotely move a compromised machine to an isolated VLAN.

## 5.2. Eradication

Once isolated, incident responders can safely begin to eliminate the threat. This may be as simple as running malware removal software or as involved as a complete wipe and restore from backup. Fewer systems in the segment means that the compromised segment or systems can be cleaned more rapidly.

## 5.3. Recovery

The affected business unit, once satisfied the threat has been eliminated, may choose to return the system to production. Once again, the micro segmentation network architecture means fewer systems are involved. The affected business unit can be brought back into production faster and it is far easier to monitor for post recovery attacks.

## 5.4. Follow-up

With the system back in production the security responders, administrators, and business personnel have a lessons learned meeting to discuss what process improvements or system changes should be made. A micro segmented network, built around well defined business processes, provides a clear and well documented foundation for this discussion. Every port, protocol, and application allowed in and out of the segment should be analyzed to determine if it is necessary. Moreover, as part of the analysis, the team should determine if additional controls or monitoring is necessary.

## 6. Emerging Trends

The architecture of the datacenter rather than the network may drive the latest wave of micro segmentation. As datacenters have evolved they have become more and more virtualized. In what has become known as the Software Defined Data Center, a logical layer of networking, compute, storage, and applications are deployed over physical infrastructure--both on premise and in the cloud. This allows businesses to rapidly provision and de-provision resources in a secure manner.

Emerging products such as VMware NSX or vArmour focus on simplifying the process of micro segmenting. Using policies or templates, these products can spin up a virtual machine, add it to a virtual switch on the correct segment, and apply firewall rules. As the case with VMware NSX, “Every virtualized workload can be protected with a full stateful firewall engine at a very granular level. Security can be based on constructs such as MAC, IP, ports, vCenter objects and tags, active directory groups, etc.” (VMware, n.d.). This allows each and every virtual machine to be segmented: the true definition of micro segmentation.

## 7. Conclusion

Organizations and their networks are constantly attacked from multiple angles and today’s defenders must use a systematic and rigorous approach to protect them. A key element to that approach is micro segmentation. Micro segmentation segregates the network in a manner that provides rapid incident response, simplified compliance, and greater visibility through continuous monitoring.

Micro segmentation begins with an understanding of the business process and how that translates into network behavior. Without that understanding, security controls will be frustrating for the users and ineffective at preventing or detecting attacks. Devices on the network are separated by their business function and security needs. Normal communication between segments is documented and any deviation from the norm should be examined.

If an incident occurs, the module nature of a segmented network simplifies the incident handling process. The segment can be rapidly isolated and the limited communication channels make determining how far the attack has spread much easier. The network and security team will have a good understanding of the business units and processes disrupted by the incident. The relationships formed through the process of understanding the necessary and normal business traffic will be invaluable during an incident. It will bring an understanding of priority and aid in the communication with the business leaders.

Micro segmentation provides value to the business in many ways beyond detecting and preventing attacks. It greatly simplifies compliance and reduces associated costs. Compliance scope can be limited and the controls are well understood and documented. Other often arduous tasks such as business continuity and disaster recovery planning benefit from the efforts of micro segmentation and vice versa. Micro segmentation affords IT an excellent opportunity to demonstrate their worth to organization. The result is a more secure, robust, and capable organization.

## References

- Arkin, O. (2007). Bypassing NAC 2.0. Retrieved January 10, 2016, from <https://www.blackhat.com/presentations/bh-dc-07/Arkin/Presentation/bh-dc-07-Arkin-ppt-up.pdf>
- Bilge, L & Dumitras, T. (2014). Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. Retrieved December 13, 2015, from [https://users.ece.cmu.edu/~tdumitra/public\\_documents/bilge12\\_zero\\_day.pdf](https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf)
- Blevins, B. (2014). Best of Data Loss Prevention 2014. *Information Security*, 16(9), 13-15.
- Byres, E. (2014). Defense-In-Depth: Reliable Security to Thwart Cyber-Attacks. *Pipeline & Gas Journal*, 241(2), 58-60.
- Cisco. (2009). Security Configuration Guide: Securing User Services. Retrieved January 3, 2016, from [http://www.cisco.com/c/en/us/td/docs/ios/sec\\_user\\_services/configuration/guide/15\\_0s/sec\\_securing\\_user\\_services\\_15\\_0S\\_book.pdf](http://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/15_0s/sec_securing_user_services_15_0S_book.pdf)
- Cisco. (2009). Cisco IOS Security Configuration Guide: Securing User Services. Retrieved January 10, 2016, from [http://www.cisco.com/c/en/us/td/docs/ios/sec\\_user\\_services/configuration/guide/15\\_0/sec\\_user\\_services\\_15\\_0\\_book.pdf](http://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/15_0/sec_user_services_15_0_book.pdf)
- Dalton, C. (2014). 7 strategies for a successful DLP strategy. Retrieved January 2, 2016, from <http://www.csoononline.com/article/2134517/strategic-planning-erm/7-strategies-for-a-successful-dlp-strategy.html>
- Duckwall, A. (2011). A Bridge Too Far: Defeating Wired 802.1x with a Transparent Bridge Using Linux. Retrieved January 10, 2016, from <https://www.defcon.org/images/defcon-19/dc-19-presentations/Duckwall/DEFCON-19-Duckwall-Bridge-Too-Far.pdf>
- Faldella, E & Tucci, P. (n.d.). Network Evasion via DNS Covert Channels. Retrieved December 16, 2015, from <https://www.primianotucci.com/media/netcross-ip-over-dns-tunneling-paper.pdf?04a20666>
- Gigamon. (2016). How to Build an Active Visibility Fabric. Retrieved January 17, 2016, from <https://www.gigamon.com/best-practices>

- Herley, C. (2014). Security, Cybercrime, and Scale. *Communications of The ACM*, 57(9), 64-71. doi:10.1145/2654847
- Kerner, S. M. (2015). Average Cost of Cyber-crime in the U.S. Rises to \$15 Million. *Eweek*, 1.
- Kershaw, M. (2011). Kismet Readme. Retrieved January 11, 2016, from <https://www.kismetwireless.net/documentation.shtml>
- Lyon, F. (2015). Firewall/IDS Evasion and Spoofing. Nmap Reference Guide. Retrieved December 12, 2015, from <https://nmap.org/book/man-bypass-firewalls-ids.html>
- Mandiant 2014 Threat Report. Retrieved December 6, 2015, from [https://dl.mandiant.com/EE/library/WP\\_M-Trends2014\\_140409.pdf](https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf)
- Martin, D. (2012). Iran behind many recent cyber attacks. Retrieved December 21, 2015, from <http://www.cbsnews.com/news/iran-behind-many-recent-cyber-attacks/>
- McAfee. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Retrieved January 2, 2016, from [http://csis.org/files/attachments/140609\\_rp\\_economic\\_impact\\_cybercrime\\_report.pdf](http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf)
- MetaGeek. (2015). What products does MetaGeek sell? Retrieved January 11, 2016, from <https://support.metageek.com/hc/en-us/articles/203686974-What-products-does-MetaGeek-sell->
- Mundhenk, D. & Rothke, B. (2007). A Guide to Practical PCI Compliance. Retrieved January 3, 2016, from <http://www.networkworld.com/article/2288753/lan-wan/a-guide-to-practical-pci-compliance.html>
- Northcutt, S. (2007). Protected Enclaves Defense-in-Depth. Retrieved December 6, 2015, from <http://www.sans.edu/research/security-laboratory/article/372>
- O'Donnell, D. (2014). Network Packet Broker: The Fastest Growing Market for Good Reason. *Wired Innovation Insights*. Retrieved January 17, 2016, from <http://insights.wired.com/profiles/blogs/network-packet-broker-the-fastest-growing-market-for-good-reason#axzz3xY4wexVj>

- Parker, M. (2015). Blended spear phishing. *SC Magazine: For IT Security Professionals* (15476693), 26(3), 11.
- PCI Security Standards Council. (2015). *Requirements and Security Assessment Procedures*. Retrieved January 16, 2016, from [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-1.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf)
- Ponemon Institute. (2011). Perceptions About Network Security: Survey of IT & IT security practitioners in the U.S. Retrieved January 2, 2016, from <http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf>
- Rome, J. (n.d.). Enclaves and Collaborative Domains. Retrieved December 5, 2015, from <http://web.ornl.gov/~webworks/cppr/y2001/pres/117259.pdf>
- Thycotic Black Hat 2014 Hacker Survey Executive Report. Retrieved December 21, 2015, from [http://thycotic.com/wp-content/uploads/2014/03/Executive-summary-blackhat-survey-data-2014\\_PDF.pdf](http://thycotic.com/wp-content/uploads/2014/03/Executive-summary-blackhat-survey-data-2014_PDF.pdf)
- VMware. (n.d.). VMware® NSX for vSphere (NSX) Network Virtualization Design Guide. Retrieved January 18, 2016, from <https://www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf>
- Zetter, K. (2015, December). Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA. *Wired*, Retrieved January 2, 2016, from <http://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/>
- Zetter, K. (2016, January). The Biggest Security Threats We'll Face in 2016. *Wired*, Retrieved January 2, 2016, from <http://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/>