

# Network Security Terms

Based on slides from [gursimrandhillon.files.wordpress.com](https://gursimrandhillon.files.wordpress.com)

# Network Security Terms

Perimeter is the fortified boundary of the network that might include the following aspects:

1. Border routers
2. Firewalls
3. IDSs
4. IPSs
5. VPN devices
6. Software architecture
7. DMZs and screened subnets

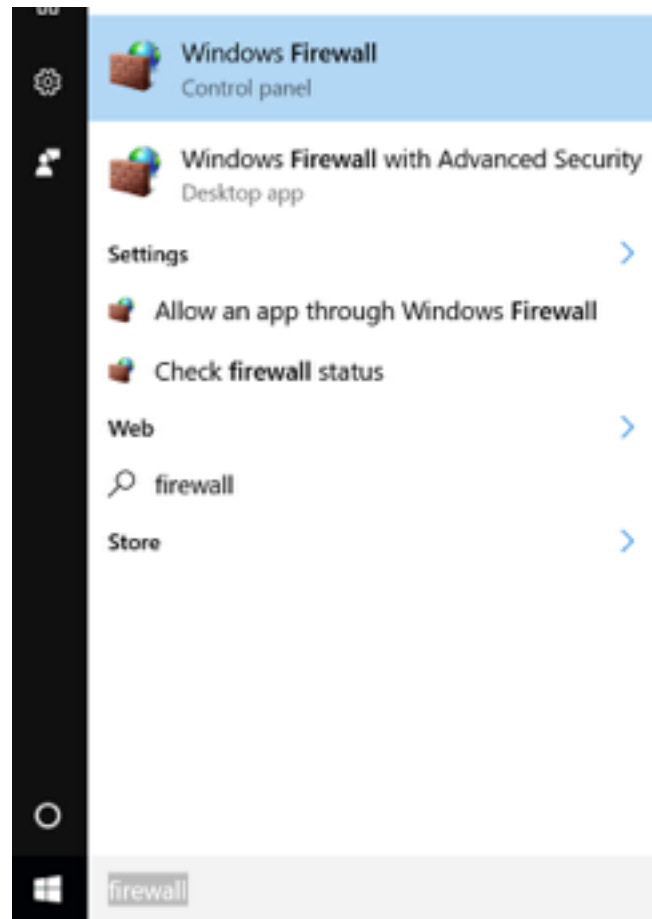
# Border Routers

1. Routers are the traffic cops of networks.
2. They direct traffic into, out of, and within our networks.
3. The border router is the last router you control before an untrusted network such as the Internet.
4. All of an organization's Internet traffic goes through this router, it often functions as a network's first and last line of defense through initial and final filtering.

# Firewalls

1. A firewall is a chokepoint device that has a set of rules specifying what traffic it will allow or deny to pass through it.
2. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic.
3. Firewalls come in several different types, including **static packet filters, stateful firewalls, and proxies.**
4. You might use a static packet filter such as a Cisco router to block easily identifiable "noise" on the Internet, a stateful firewall such as a Check Point FireWall-1 to control allowed services, or a proxy firewall such as Secure Computing's Sidewinder to control content.
5. Although firewalls aren't perfect, they do block what we tell them to block and allow what we tell them to allow.

# Windows Firewall



# Windows Firewall

The screenshot shows the Windows Firewall control panel window. The title bar reads "Windows Firewall". The breadcrumb navigation path is "Control Panel > System and Security > Windows Firewall".

**Left sidebar:**

- Control Panel Home
- Allow an app or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

**Main content area:**

## Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

[What are the recommended settings?](#)

[Use recommended settings](#)

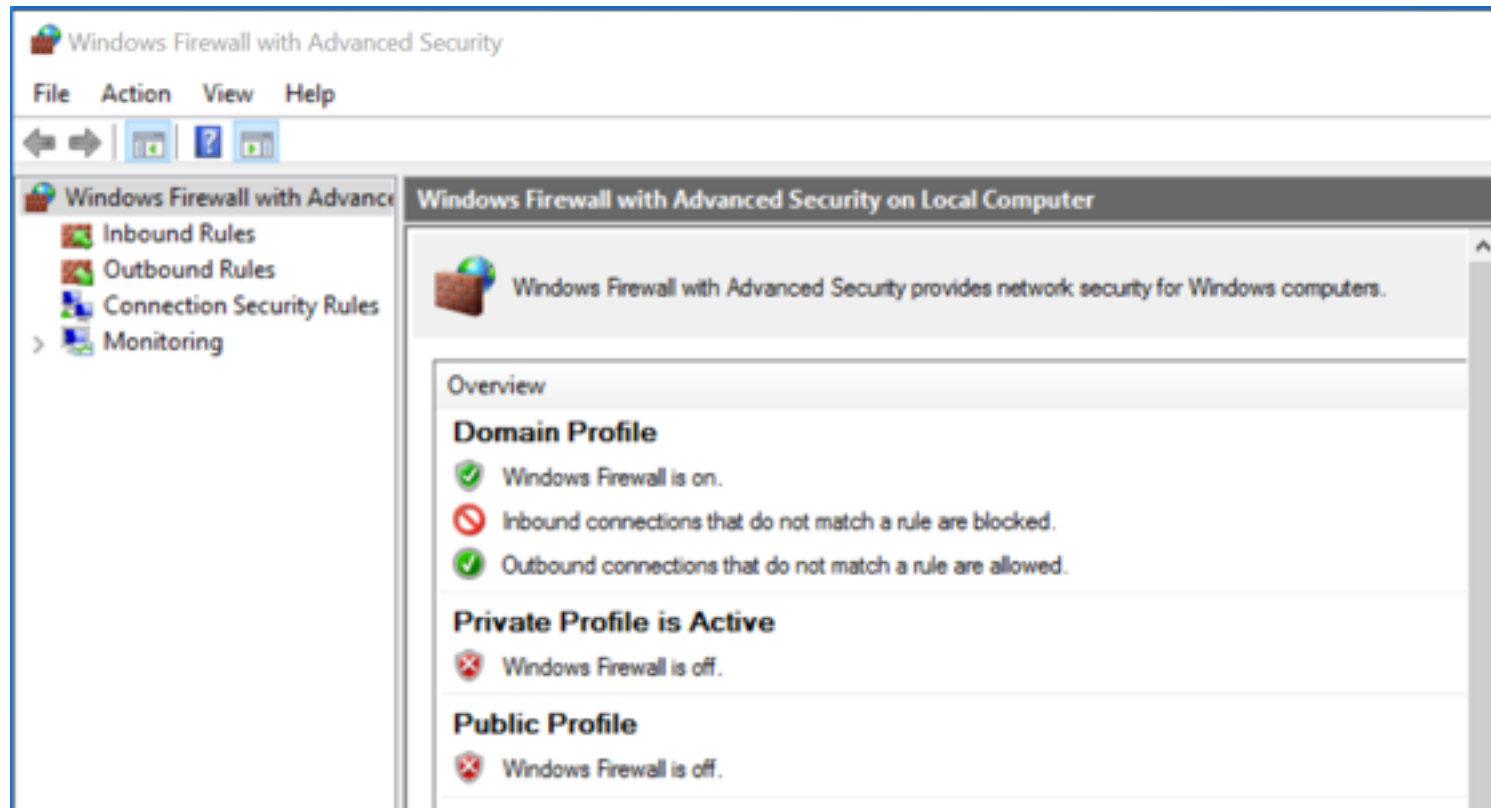
### Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

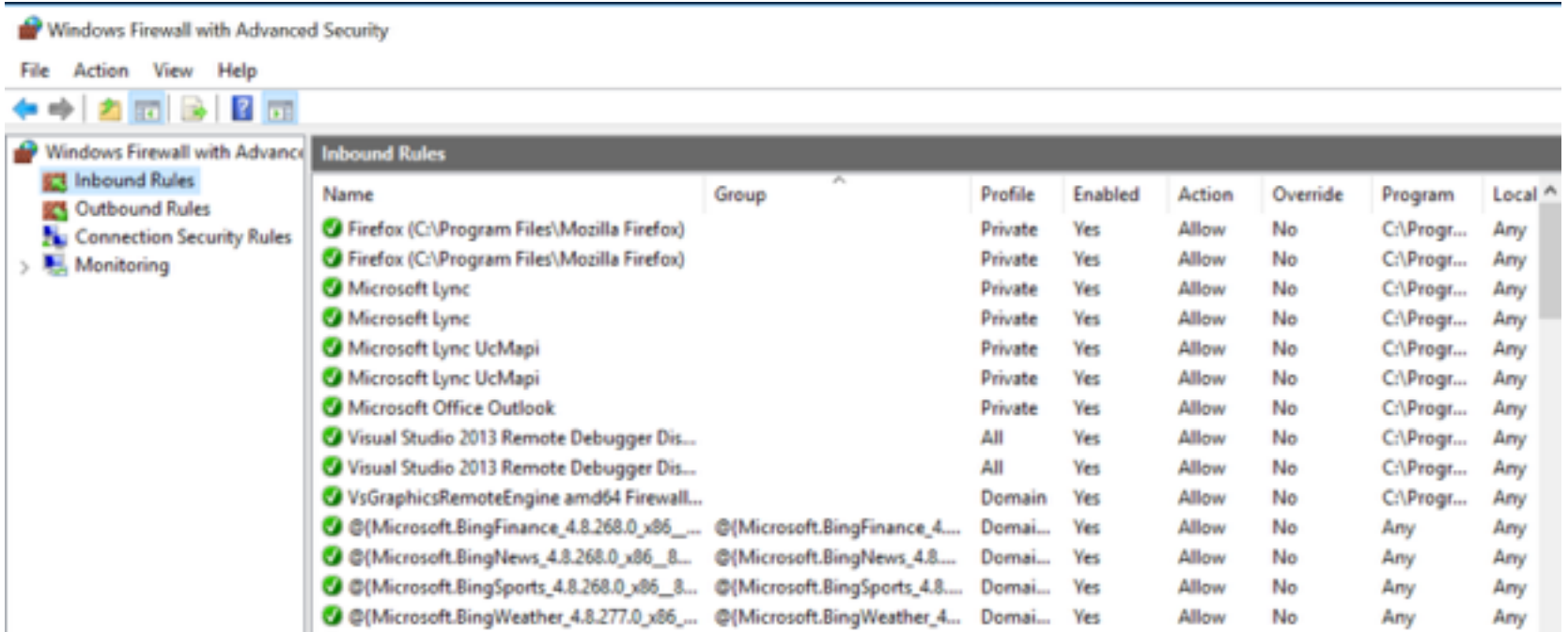
Windows Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new app

### Guest or public networks Not connected

# Firewall Profiles



# Incoming Rules



The screenshot displays the Windows Firewall with Advanced Security console. The left-hand pane shows a tree view with 'Inbound Rules' selected. The main pane shows a list of inbound rules with the following columns: Name, Group, Profile, Enabled, Action, Override, Program, and Local. The rules listed include Firefox, Microsoft Lync, Microsoft Office Outlook, Visual Studio 2013 Remote Debugger, and various Bing services.

Name	Group	Profile	Enabled	Action	Override	Program	Local
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progr...	Any
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progr...	Any
✓ Microsoft Lync		Private	Yes	Allow	No	C:\Progr...	Any
✓ Microsoft Lync		Private	Yes	Allow	No	C:\Progr...	Any
✓ Microsoft Lync UcMapi		Private	Yes	Allow	No	C:\Progr...	Any
✓ Microsoft Lync UcMapi		Private	Yes	Allow	No	C:\Progr...	Any
✓ Microsoft Office Outlook		Private	Yes	Allow	No	C:\Progr...	Any
✓ Visual Studio 2013 Remote Debugger Dis...		All	Yes	Allow	No	C:\Progr...	Any
✓ Visual Studio 2013 Remote Debugger Dis...		All	Yes	Allow	No	C:\Progr...	Any
✓ VsGraphicsRemoteEngine amd64 Firewall...		Domain	Yes	Allow	No	C:\Progr...	Any
✓ @({Microsoft.BingFinance_4.8.268.0_x86_...	@({Microsoft.BingFinance_4...	Domai...	Yes	Allow	No	Any	Any
✓ @({Microsoft.BingNews_4.8.268.0_x86_8...	@({Microsoft.BingNews_4.8...	Domai...	Yes	Allow	No	Any	Any
✓ @({Microsoft.BingSports_4.8.268.0_x86_8...	@({Microsoft.BingSports_4.8...	Domai...	Yes	Allow	No	Any	Any
✓ @({Microsoft.BingWeather_4.8.277.0_x86_...	@({Microsoft.BingWeather_4...	Domai...	Yes	Allow	No	Any	Any



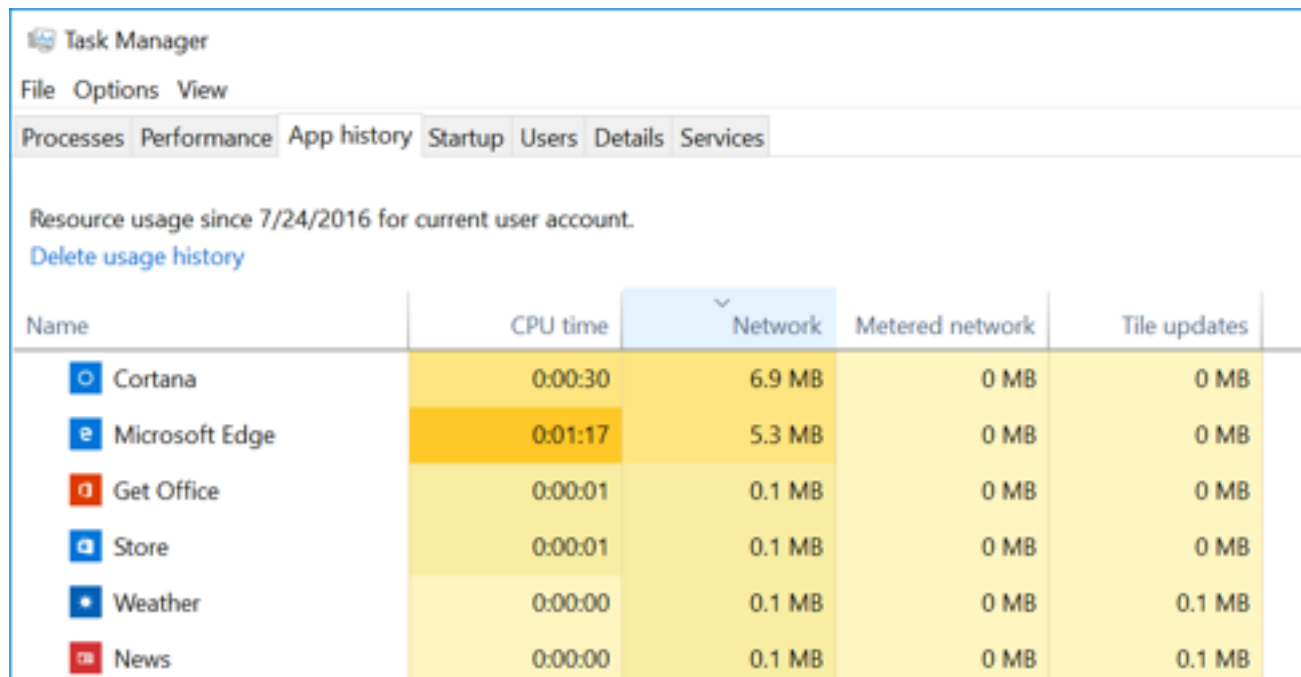
# netstat

```
Command Prompt
C:\Users\Admin2>netstat -an | more

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP   0.0.0.0:7680             0.0.0.0:0               LISTENING
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49666            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49667            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49671            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49678            0.0.0.0:0               LISTENING
TCP   0.0.0.0:50550            0.0.0.0:0               LISTENING
TCP   172.16.1.138:139        0.0.0.0:0               LISTENING
TCP   172.16.1.138:50953      184.25.56.173:80        TIME_WAIT
TCP   172.16.1.138:50956      184.25.56.173:80        TIME_WAIT
TCP   172.16.1.138:50960      40.83.182.229:80        TIME_WAIT
TCP   172.16.1.138:50963      23.5.251.27:80          TIME_WAIT
TCP   172.16.1.138:50980      23.101.14.229:443       TIME_WAIT
TCP   172.16.1.138:50981      168.61.149.17:443       TIME_WAIT
TCP   172.16.1.138:50986      64.4.54.254:443         TIME_WAIT
TCP   172.16.1.138:50993      207.46.114.58:443       TIME_WAIT
TCP   172.16.1.138:50994      8.254.207.94:80         ESTABLISHED
TCP   172.16.1.138:50995      8.254.207.94:80         ESTABLISHED
TCP   172.16.1.138:50996      8.254.207.94:80         ESTABLISHED
TCP   172.16.1.138:50997      8.254.207.94:80         ESTABLISHED
```

# Task Manager









Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Resource usage since 7/24/2016 for current user account.  
[Delete usage history](#)

Name	CPU time	Network	Metered network	Tile updates
 Cortana	0:00:30	6.9 MB	0 MB	0 MB
 Microsoft Edge	0:01:17	5.3 MB	0 MB	0 MB
 Get Office	0:00:01	0.1 MB	0 MB	0 MB
 Store	0:00:01	0.1 MB	0 MB	0 MB
 Weather	0:00:00	0.1 MB	0 MB	0.1 MB
 News	0:00:00	0.1 MB	0 MB	0.1 MB

# Resource Monitor

Resource Monitor

File Monitor Help

Overview CPU Memory Disk Network

**Processes with Network Activity**

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
wermgr.exe	3680	839	692	1,531
NIS.exe	1708	119	398	517
svchost.exe (ulcsvc)	972	235	49	283
svchost.exe (NetworkService)	1168	94	38	132
System	4	57	0	57
OfficeClickToRun.exe	1880	0	30	30
svchost.exe (LocalServiceNet...)	1228	10	0	10
svchost.exe (netvcs)	1176	3	5	8

**Network Activity** 1 Kbps Network I/O 0% Network Utilization

**TCP Connections**

Image	PID	Local Addr...	Local Port	Remote A...	Remote Port	Packet Los...	Latency (ms)
svchost.exe (ulcsvc)	972	172.16.1.1...	51022	64.4.54.254	443	0	6
wermgr.exe	3680	172.16.1.1...	51035	65.52.108...	443	0	0
NIS.exe	1708	172.16.1.1...	51034	166.98.6.31	443	-	-
-	-	172.16.1.1...	51030	134.170.5...	443	-	-
MpCmdRun.exe	1340	172.16.1.1...	51029	191.238.2...	443	-	-
svchost.exe (netvcs)	1176	172.16.1.1...	51027	157.55.24...	443	-	-
OfficeClickToRun.exe	1880	172.16.1.1...	51024	23.101.14...	443	0	-
-	-	172.16.1.1...	51023	64.4.54.18	443	-	-
svchost.exe (netvcs)	1176	172.16.1.1...	51021	13.107.4.50	80	-	-

**Listening Ports**

Image	PID	Address	Port	Protocol	Firewall Status
svchost.exe (LocalService)	1256	IPv6 unspecified	123	UDP	Allowed, restri...
svchost.exe (LocalService)	1256	IPv4 unspecified	123	UDP	Allowed, restri...
svchost.exe (RPCSS)	928	IPv6 unspecified	135	TCP	Allowed, not r...
svchost.exe (RPCSS)	928	IPv4 unspecified	135	TCP	Allowed, not r...
System	4	172.16.1.138	137	UDP	Allowed, not r...
System	4	172.16.1.138	138	UDP	Allowed, not r...
System	4	172.16.1.138	139	TCP	Allowed, not r...
System	4	IPv6 unspecified	445	TCP	Allowed, not r...
System	4	IPv4 unspecified	445	TCP	Allowed, not r...

**Views**

- Network: 10 Kbps (60 Seconds)
- TCP Connections: 20
- Ethernet0: 100%
- Bluetooth Network Con...: 100%

# Ubuntu: ufw

```
student@ubuntu:~$ sudo ufw enable
[sudo] password for student:
Firewall is active and enabled on system startup
student@ubuntu:~$ sudo ufw disable
Firewall stopped and disabled on system startup
student@ubuntu:~$ █
```

# Kali: iptables

```
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                               destination
root@kali:~# iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                               destination
DROP      tcp  --  anywhere                             anywhere          tcp flags:RST/RST
root@kali:~#
```

# Intrusion Detection Systems

1. An IDS is like a burglar alarm system for your network that is used to detect and alert on malicious events.
2. The system might comprise many different IDS sensors placed at strategic points in your network.
3. Two basic types of IDS exist: **network-based (NIDS)**, such as **Snort or Cisco Secure IDS**, and **host-based (HIDS)**, such as **Tripwire or ISS BlackICE**.
4. NIDS sensors monitor network traffic for suspicious activity. NIDS sensors often reside on subnets that are directly connected to the firewall, as well as at critical points on the internal network. HIDS sensors reside on and monitor individual hosts.

# Intrusion Detection Systems

5. In general, IDS sensors watch for predefined signatures of malicious events, and they might perform statistical and anomaly analysis.
6. When IDS sensors detect suspicious events, they can alert in several different ways, including email, paging, or simply logging the occurrence.
7. IDS sensors can usually report to a central database that correlates their information to view the network from multiple points.

# Snort

← → ↻ 🏠 <https://samsclass.info/122/proj/120-p15-snort.html>

## **Project 15 for CNIT 120 - Snort (15 pts.)**

- Link Per 1



# Intrusion Prevention Systems

- An IPS is a system that automatically detects and stops computer attacks against protected resources.
- An IPS strives to automatically defend the target without the administrator's direct involvement. Such protection may involve using signature-based or behavioral techniques to identify an attack and then blocking the malicious traffic or system call before it causes harm.
- In this respect, an IPS combines the functionality of a firewall and IDS to offer a solution that automatically blocks offending actions as soon as it detects an attack.
- Some IPS products exist as standalone systems, such as TippingPoint's UnityOne device. Additionally, leading firewall and IDS vendors are incorporating IPS functionality into their existing products.

# Virtual Private Networks

1. A VPN is a protected network session formed across an unprotected channel such as the Internet.
2. Frequently, we reference a VPN in terms of the device on the perimeter that enables the encrypted session, such as Cisco VPN Concentrator.
3. A VPN allows an outside user to participate on the internal network as if connected directly to it.
4. Many organizations have a false sense of security regarding their remote access just because they have a VPN.
5. However, if an attacker compromises the machine of a legitimate user, a VPN can give that attacker an encrypted channel into your network.

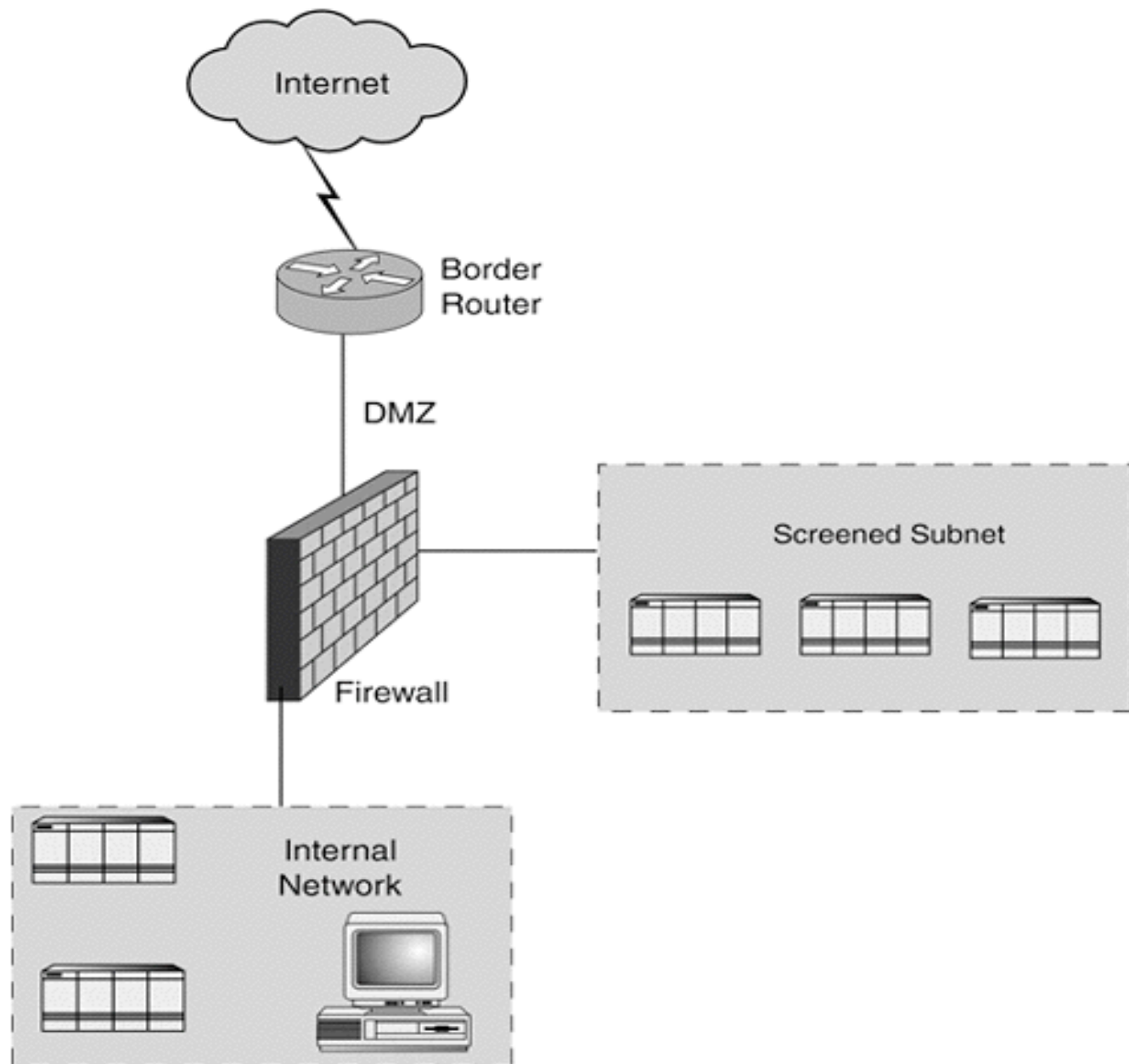
# Software Architecture

Software architecture refers to applications that are hosted on the organization's network, and it defines how they are structured. For example, we might structure an e-commerce application by splitting it into three distinct tiers:

1. The web front end that is responsible for how the application is presented to the user
2. The application code that implements the business logic of the application
3. The back-end databases that store underlying data for the application

# De-Militarized Zones and Screened Subnets

1. We typically use the terms DMZ and screened subnet in reference to a small network containing public services connected directly to and offered protection by the firewall or other filtering device.
2. The term DMZ originated during the Korean War when a strip of land at the 38th parallel was off-limits militarily. A DMZ is an insecure area between secure areas. Just as the DMZ in Korea was in front of any defenses, the DMZ, when applied to networks, is located outside the firewall.
3. A firewall or a comparable traffic-screening device protects a screened subnet that is directly connected to it. Remember this: A DMZ is in front of a firewall, whereas a screened subnet is behind a firewall.



https://www.phantom.us

Phantom

OVERVIEW PRODUCT BLOG GET PHANTOM NOW MY PHANTOM

RSAC Innovation Sandbox 2016 WINNER

CRN 10 COOLEST SECURITY STARTUPS 2016

1ST PURPOSE-BUILT  
COMMUNITY-POWERED  
**SECURITY AUTOMATION &  
ORCHESTRATION**

Link Per 5