15º SEMINÁRIO DE AUTOMAÇÃO E TI INDUSTRIAL 2011
15th AUTOMATION AND INDUSTRIAL IT SEMINAR
ISSN 2237-0234
ABM
20 a 22 de setembro 2011 - São Paulo - SP

MELHORIA DA POLÍTICA DE SEGURANÇA DAS REDES DE CONTROLE DE PROCESSO DA ARCELORMITTAL TUBARÃO[1]

Leonardo Silva Nunes[2]
Antônio Carlos Aguiar Gagno Júnior[2]

Resumo
Com o crescimento contínuo das soluções de controle, gerenciamento e monitoração, suportadas através de redes ethernet e, principalmente, baseadas em padrões comerciais, como o TCP-IP, é cada vez mais exigido das empresas aderirem a recursos tecnológicos para aprimoramento da segurança da informação e, assim, incorporar um diferencial aos seus processos de fabricação. Nesse contexto, as redes de controle passam a ser utilizadas para recebimento de tráfego não apenas inerente a controle, mas também monitoração, gerenciamento, engenharia (*downloads* e *uploads*), controle de manutenção (calibração, histórico, tendência, impedimentos), dentre outros. É, portanto, necessário realizar alguns controles objetivando garantir o desempenho e confiabilidade requeridos para a segurança da informação da empresa. A esse conjunto de ações dá-se o nome de Segurança de Rede de Controle de Processo.
Palavras-chave: Comunicação de dados; Rede de controle de processo; Protocolo TCP-IP; *Ethernet*.

IMPROVEMENT OF THE ARCELORMITTAL TUBARÃO NETWORK PROCESS CONTROL SECURITY POLICY

Abstract
With the continuous growth of the control, management and monitoring solutions supported through Ethernet network and mainly based on commercial standards, such as the TCP-IP, it's increasingly demanded from the companies adhere to technological resources to improve information security and thus incorporate a differential to their manufacturing processes. In this sense, control networks are now used to receiving the traffic not only inherent in control, but also monitoring, management, engineering (downloads and uploads), maintenance control (calibration, historic, trends, impediments), among others. It is therefore necessary to make some controls aiming to guarantee the required performance and reliability for the security of enterprise information. This group of action I called Network Security Process Control.
Key words: Data communication; Network process control; TCP-IP Protocol; Ethernet.

[1] *Contribuição técnica ao 15° Seminário de Automação e TI Industrial, 20 a 22 de setembro de 2011, São Paulo, SP.*
[2] *Especialista em Desenvolvimento de Automação e Instrumentação, ArcelorMittal Tubarão.*

ISSN 2237-0234
ABM ASSOCIAÇÃO BRASILEIRA DE METALURGIA, MATERIAIS E MINERAÇÃO
20 a 22 de setembro 2011 - São Paulo - SP

1 INTRODUÇÃO

Devido ao grande aumento das aplicações de controle de processo em ambiente de rede e, principalmente, devido às vulnerabilidades existentes, considerando o uso por essas aplicações de plataformas de propósitos gerais, como por exemplo microcomputadores com sistema operacional Windows e protocolo de comunicação TCP-IP, com ampla conectividade para dentro e fora da empresa, a ArcelorMittal Tubarão tem investido em metodologias e implementações de políticas de segurança para garantia de desempenho e disponibilidade de seus sistemas de controle de processo.
As atividades nesse sentido iniciaram com o levantamento das vulnerabilidades e necessidades de todas as plantas da Usina, o estudo das tecnologias protetivas disponíveis considerando a preservação do investimento dos ativos de redes já existentes. A partir daí foram definidas as linhas de atuação.
Com a implantação de ativos de rede que aderem aos padrões abertos ISO/OSI, toda a política é baseada em redes locais com isolamento e conectividade controlada, baseada em listas de controle de acesso, bloqueios de tráfegos desnecessários, controle de intensidade, priorização de tráfego, dentre outros.
Todos os segmentos de rede de comunicação de dados são monitorados continuamente e os dados são armazenados para análise posterior, se necessário, por meio de uma plataforma centralizada de gerenciamento e monitoração.

2 OBJETIVO

Com o objetivo de suprir a crescente implantação de sistemas de controle em rede com níveis seguros de desempenho e alta disponibilidade, a ArcelorMittal Tubarão implantou dois Sistemas, sendo um de monitoração e outro de gerenciamento de todos os *links* e equipamentos de redes de dados de controle de processo a partir de Plataformas Centrais de Aquisição e Armazenamento de Dados.
Estas Plataformas Centrais permitem a supervisão, monitoramento *on-line* e o gerenciamento centralizado das principais ameaças à segurança dos segmentos de comunicação, possibilitando a análise de tráfegos, sinalização e alarmes, bem como o bloqueio de acesso e filtro de tráfego.

3 CENÁRIO INICIAL DAS REDES DE PROCESSO

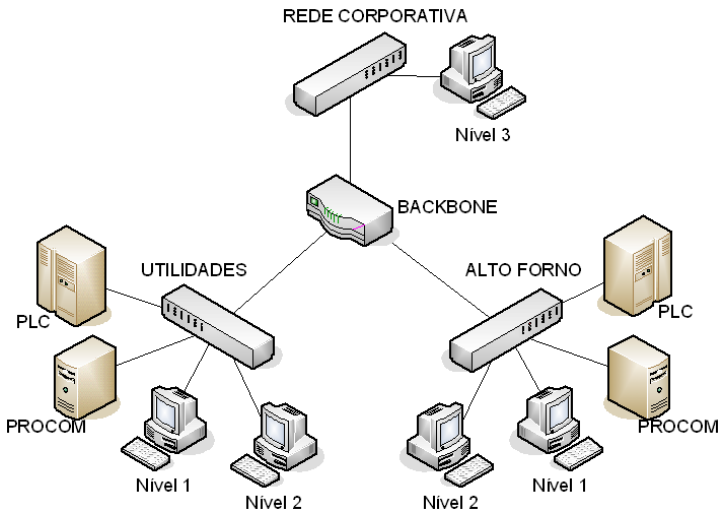
Os itens a seguir apresentam as necessidades operacionais das redes de controle de processo da ArcelorMittal Tubarão, as soluções de mercado utilizadas para atender tais necessidades, os problemas identificados e as ocorrências provocadas por esses problemas. O cenário inicial pode ser observado na Figura 1.
Necessidades operacionais:

- redes baseadas na interconectividade;
- alto desempenho; e
- alta disponibilidade (24x7).

ISSN 2237-0234
ABM ASSOCIAÇÃO BRASILEIRA DE METALURGIA, MATERIAIS E MINERAÇÃO
20 a 22 de setembro 2011 - São Paulo - SP

Soluções implantadas:

- padrão *Ethernet*;
- gerenciamento de redes utilizando a ferramenta CiscoWorks
- monitoração de redes pelo sistema Nagios, otimizado conforme as necessidades da ArcelorMittal Tubarão;
- rotas fixas; e
- redundância entre *links*.



Fonte: ArcelorMittal Tubarão
Figura 1. Cenário Inicial da rede de controle de processo da ArcelorMittal Tubarão.

Problemas identificados:

- tráfego indesejado;
- queda de desempenho da rede;
- propagação de *malwares*; e
- falta de controle de acesso.

Ocorrências:

- infecção de plataformas Microsoft por *malwares*;
- estouro de buffer em PLC´s;
- l*oop* entre rede corporativa e de controle de processos no LTQ; e
- alterações no *Spanning Tree Protocol* (STP) na rede corporativa impactaram estabilidade da rede de controle de processos.

4 POLITICA DE SEGURANÇA

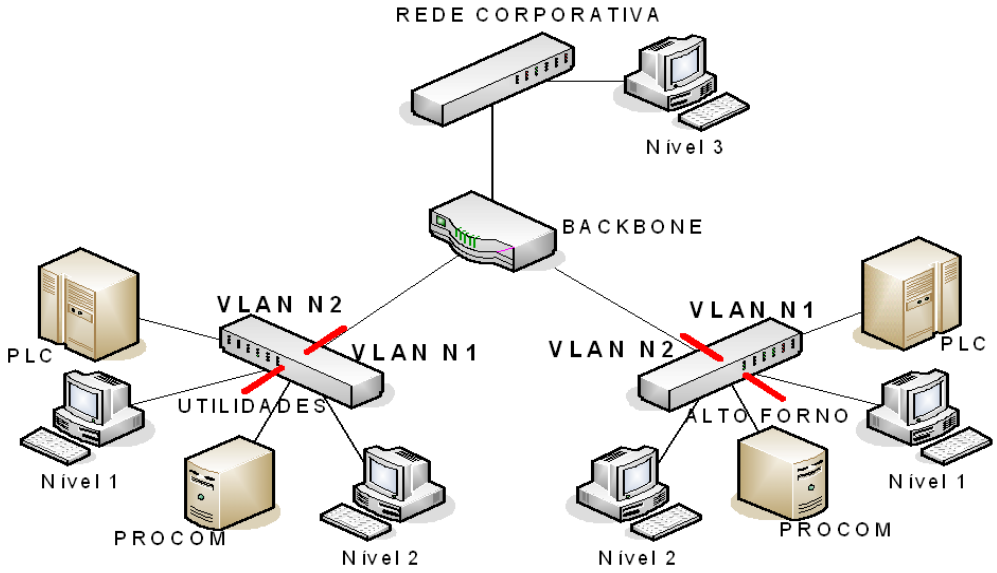
4.1 Descrição

A Política de segurança das redes de controle de processo da ArcelorMittal Tubarão objetiva planejar o tratamento dos itens:

- controle de acesso indevido (autenticação centralizada, controladores de domínio, políticas de autenticação, senhas fracas, expiração de senhas, dentre outros);
- compartilhamento de recursos (políticas de acesso a recursos de rede);

- ameaças virtuais (vírus, *trojans*, *phishing*, *spyware*, atualizações para sistemas operacionais, WSUS, soluções antivírus: *Symantec Corporate Edition*);
- propagação indevida (*broadcasts*, anúncio de serviços, definição de rotas, redução do domínio de *broadcasts*, redes virtuais, controle de pacotes);
- estabilidade da configuração x redundância (*Loop*, *Spanning Tree Protocol*, rotas, desempenho);
- habilitação de recursos (*Access List*, *Radius server*, controle de interfaces, filtro de portas TCP);
- engargalamento de *buffer* (*timeout* em resposta de PLC's).
- a política de segurança da ArcelorMittal Tubarão é baseada nos seguintes recursos:
- monitoração contínua através de consultas via protocolo SNMP;
- armazenamento e apresentação dos dados coletados;
- emissão de alarmes e mensagens de alerta;
- geração de relatórios semanais para controle do desempenho dos segmentos de rede;
- configuração dos ativos de rede para confinamento de tráfego, listas de controle de acesso, bloqueios de tráfegos desnecessários, controle de intensidade e priorização de tráfego, dentre outros.
- configuração de estações de trabalho para evitar acessos indevidos, propagação indevida de arquivos, acessos a mídias removíveis, etc.
- atualização sistematizada das plataformas e sistemas operacionais de forma a minimizar as vulnerabilidades dos sistemas conforme as recomendações dos fabricantes;
- campanhas educativas de utilização de recursos de informática; e
- inventários e auditorias periódicas e aleatórias nos sistemas e ativos de redes e de informática para monitoração, controle e garantia da política de segurança.

A Figura 2 apresenta o recurso de confinamento de tráfego através de implementação de VLAN.



Fonte: ArcelorMittal Tubarão

Figura 2. Segmentação isolando as redes de controle de processo da ArcelorMittal Tubarão.

ISSN 2237-0234
ABM ASSOCIAÇÃO BRASILEIRA DE METALURGIA, MATERIAIS E MINERAÇÃO
20 a 22 de setembro 2011 - São Paulo - SP

4.2 Implantação da Política de Segurança

4.2.1 Primeira fase

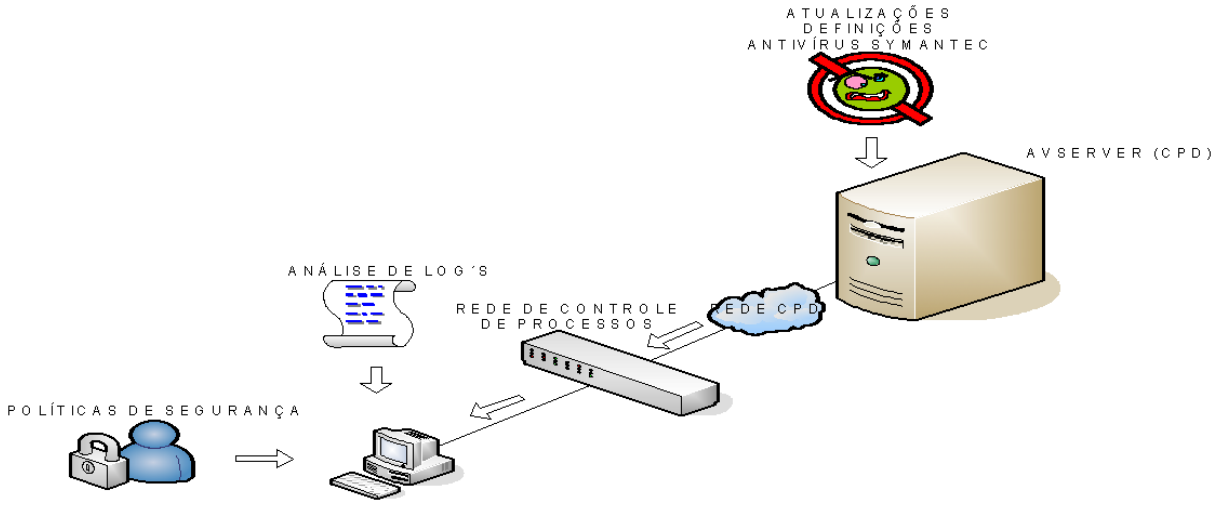
Na primeira fase da Política de Segurança de Redes de Controle de Acesso da ArcelorMittal Tubarão foram implementadas as seguintes melhorias:

- aprimoramento de ativos do *backbone* da ArcelorMittal Tubarão;
- bloqueio de portas TCP entre rede de controle de processos e rede corporativa;
- bloqueio de pacotes, implementação de filtro para pacotes RPC;
- eliminação de *bridging* entre portas; e
- melhor controle de tráfego da rede.

4.2.2 Segunda fase

- Segmentação de redes, divisão da rede em segmentos lógicos de nível 1 e 2;
  - vantagens: redução do domínio de *broadcasts*; isolamento do segmento de tráfego indesejado; otimização da performance da rede no segmento virtual; e
  - desvantagens: isolamento de redes que requerem conectividade com outras redes.
- *access list*: aumento de segurança na rede; controle de tráfego entre os nós; maior demanda de processamento dos ativos de rede.
- análise de l*ogs*: análise de *logs* para identificação de possíveis distúrbios de *hardware* e *software*.
- políticas de segurança nas estações de trabalho: aplicação local de políticas de segurança; atualização de plataformas Microsoft durante manutenção das estações; padronização de todo o parque de estações de processo, clonagem das estações de trabalho.
- solução antivírus: implantada solução antivírus, adotada pelo setor de TI na rede corporativa, com adequações para as aplicações das redes de processo. Aplicação da solução *Symantec Corporate Edition* para atendimento à complexidade do ambiente.

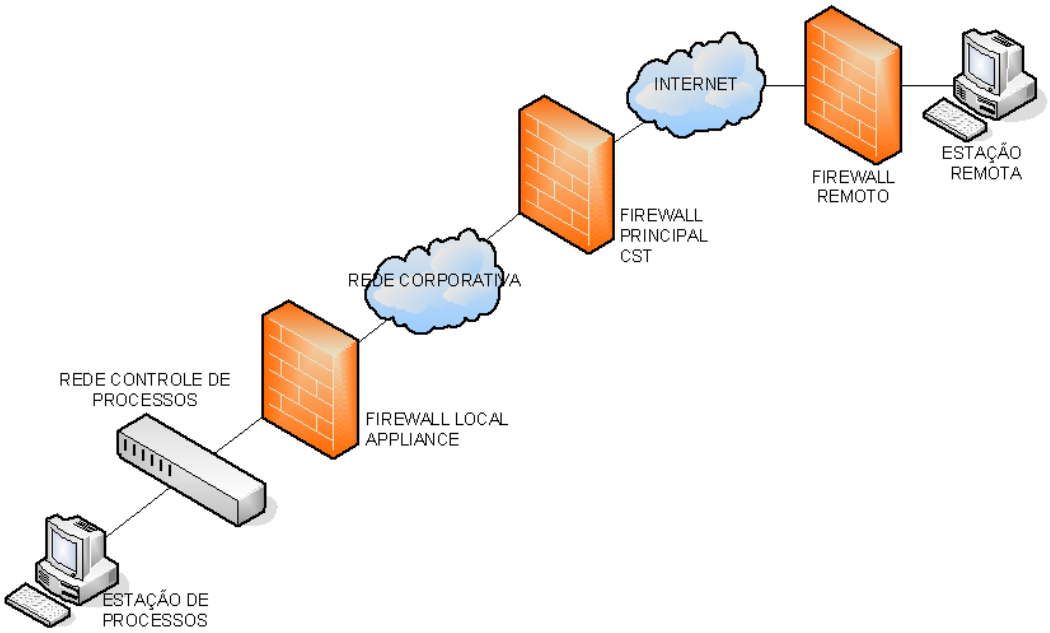
A Figura 3 apresenta o recurso de política de segurança para as estações de trabalho.



Fonte: ArcelorMittal Tubarão
Figura 3. Política de segurança para estações de trabalho.

ISSN 2237-0234
ABM ASSOCIAÇÃO BRASILEIRA DE METALURGIA, MATERIAIS E MINERAÇÃO
20 a 22 de setembro 2011 - São Paulo - SP

A Figura 4 apresenta o recurso de política de segurança para acesso remoto às redes de controle de processo da ArcelorMittal Tubarão.



Fonte: ArcelorMittal Tubarão
Figura 4. Política de segurança para acesso remoto (via VPN).

4.2.3 Fase atual

- Substituição do sistema de monitoração de redes pelo Nagios, via SNMP;
- implementação do sistema de gerenciamento CiscoWorks;
- controle de acesso dos equipamentos de rede com *login* e senha individual; e
- em estudo o isolamento das redes de processo com a rede corporativa, viabilizando o tráfego entre as mesmas apenas via *firewall*.

5 RESULTADOS

A implantação da política de segurança nas redes de controle de processo na ArcelorMittal Tubarão possibilita ganhos de desempenho expressivos, tais como:

- redução significativa das ocorrências indesejáveis nos segmentos de redes de controle de processo não impactando na variabilidade dos processos produtivos;
- aperfeiçoamento do controle dos ativos de Informática da empresa em função da otimização da avaliação dos processos operacionais e sistemas de otimização e controle, permitindo ações preventivas e corretivas imediatas;
- integração das equipes de operação, manutenção e desenvolvimento nas discussões e avaliações dos resultados do monitoramento contínuo e dos impactos da empresa;
- orientação das ações de manutenção de forma a priorizar as intervenções nos sistemas de otimização e controle e processos produtivos; e
- geração de um banco de dados eficiente para realização de análises estatísticas da influência das implantações de melhorias e de expansões.

ISSN 2237-0234
ABM ASSOCIAÇÃO BRASILEIRA DE METALURGIA, MATERIAIS E MINERAÇÃO
20 a 22 de setembro 2011 - São Paulo - SP

6 CONCLUSÃO

A ArcelorMittal Tubarão cumpre com as diretrizes de sua política de segurança da informação que têm como foco “buscar a melhoria contínua e a prevenção de ocorrências de falha” e se antecipar às demandas de melhorias e expansões de seus sistemas de controle de processo de produção. Conclui-se ainda que a política implantada tenha parcela significativa na:

- redução das ocorrências de falhas na empresa em função do aprimoramento dos processos e implantação de melhorias nos procedimentos e equipamentos; e
- contribuição para melhoria do desempenho com aumento da confiabilidade e da disponibilidade dos sistemas de otimização e controle de processo de produção.

BIBLIOGRAFIA

1 ROSE, Marshall T. *How to manage your network using SNMP*. Prentice Hall, 1995.
2 MAGGIORA, P.L.D. *Performance and fault management*. Cisco Press, 2000.
3 JONES, Edmond D. *Information Security Police Manual*. Rothstein Associates; 2001.
4 Manuais dos Ativos de Rede Cisco, 2010.
5 Padrões Técnicos e Padrões de Operação da ArcelorMittal Tubarão para Segurança da Informação, 2010.